

ICS 33.050
CSS M 30

团 体 标 准

T/TAF 123—2022



软件开发包（SDK）个人信息处理规范

Processing specification for personal information of software
development kit (SDK)

2022-11-25 发布

2022-11-25 实施

电信终端产业协会 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 总体要求	2
5.1 SDK 处理个人信息框架	2
5.2 SDK 处理个人信息原则	3
5.3 SDK 提供者与 SDK 使用者双方义务	3
6 个人信息处理各环节要求	3
6.1 个人信息收集要求	4
6.2 个人信息存储要求	5
6.3 个人信息使用要求	5
6.4 个人信息加工要求	6
6.5 个人信息传输要求	6
6.6 个人信息对外提供要求	6
6.7 个人信息公开要求	6
6.8 个人信息删除要求	6
6.9 个人信息跨境要求	7
7 用户权利保障	7
8 SDK 提供者要求	7
9 评估方法	8
9.1 个人信息处理各环节的评估	8
9.2 用户权利保障的评估	16
9.3 SDK 提供者的评估	17

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、北京字节跳动网络技术有限公司、阿里巴巴(中国)有限公司、北京快手科技有限公司、每日互动股份有限公司、郑州信大捷安信息技术股份有限公司、小米科技有限责任公司、荣耀终端有限公司、高通无线通信技术(中国)有限公司、北京三星通信技术研究有限公司、博鼎实华(北京)技术有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、华为技术有限公司、北京三快在线科技有限公司、北京奇虎科技有限公司、中兴通讯股份有限公司、深圳市腾讯计算机系统有限公司、广州虎牙信息科技有限公司、上海兆言网络科技有限公司。

本文件主要起草人：武林娜、宋恺、刘陶、王艳红、杜云、王淞鹤、王宇晓、李昳婧、贾雪飞、黄天宁、方强、于洋、落红卫、王昕、董霖、方毅、刘献伦、刘为华、顾泽宇、赵晓娜、王江胜、吴越、董霁、付艳艳、贾科、徐曼、衣强、李实、王芳、祖岩岩、姚一楠、张宏伟、徐永太、蔡倩文、郑云、王平、曾雅静、张贝贝、赵乃萱、张吉、李巨、田泽宇、姜宇栋。



引 言

本文件根据《中华人民共和国个人信息保护法》等相关法律要求，针对软件开发包（SDK）提出了个人信息处理要求，进一步促进移动互联网行业的健康稳定发展。



软件开发包（SDK）个人信息处理规范

1 范围

本文件规定了对外提供服务的软件开发包（SDK）个人信息处理规范，包括软件开发包（SDK）处理个人信息的基本要求、软件开发包（SDK）提供者的基本要求以及保障及时响应用户权利的要求。

本文件适用于软件开发包（SDK）提供者对个人信息处理活动进行设计、开发和评估，也适用于主管部门、第三方评估机构等组织对软件开发包的个人信息处理行为进行监督、管理和评估。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动互联网应用程序 application

可安装在移动智能终端内，能够利用移动智能终端操作系统提供的公开开发接口，实现某项或某几项特定任务的应用程序。

注：包含移动智能终端预置应用、小程序、快应用以及互联网信息服务提供者提供的可以通过网站、应用商店等应用分发平台下载、安装、升级的应用程序，简称 APP。

3.2

软件开发包使用者 software development kit user

将 SDK 集成到自身产品并决定该产品的开发、运营、个人信息处理、数据安全管理等活动的目的和方式的组织或个人，简称 SDK 使用者。

3.3

软件开发包 software development kit

协助软件开发的软件库，包括相关的代码、文档、范例和工具的集合。

3.4

软件开发包提供者 software development kit provider

决定 SDK 的开发、运营、个人信息处理、数据安全管理等活动的目的和方式的组织或个人，简称 SDK 提供者。SDK 提供者提供的内容不只是简单的 SDK 工具包，还有为了实现相关功能与之配套的平台能力。

3.5

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

3.6

敏感个人信息 sensitive personal information

一旦泄露或者非法使用,可能导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。

3.7

敏感权限 sensitive permissions

是移动智能终端对系统敏感资源的一种管控方式,通常简称为敏感权限。敏感权限管控范围涵盖应用程序所涉及用户敏感个人信息的受限数据或资源的区域,或者可能会影响用户存储的数据或其他应用软件的操作。

注:敏感权限通常由APP向移动智能终端系统作出权限申请,用户授权后访问。

3.8

自动化决策 automated decision

通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等,并进行决策的活动。

4 缩略语

下列缩略语适用于本文件。

APP: 移动应用软件 (Application)

SDK: 软件开发包 (Software Development Kit)

5 总体要求

5.1 SDK 处理个人信息框架

SDK使用者一般会在宿主程序的基础上集成若干SDK提供者提供的SDK,SDK使用者与SDK提供者个人信息保护责任划分包括以下三种情况:

- a) SDK提供者独立处理个人信息的,应自行承担个人信息保护责任;
- b) SDK提供者受SDK使用者委托或与SDK使用者共同处理个人信息的,可按照合作协议或共同协商各自承担的责任;
- c) 当SDK使用者独立处理个人信息的,应由SDK使用者承担个人信息保护的责任。

SDK处理个人信息数据流转框架图如图1所示。

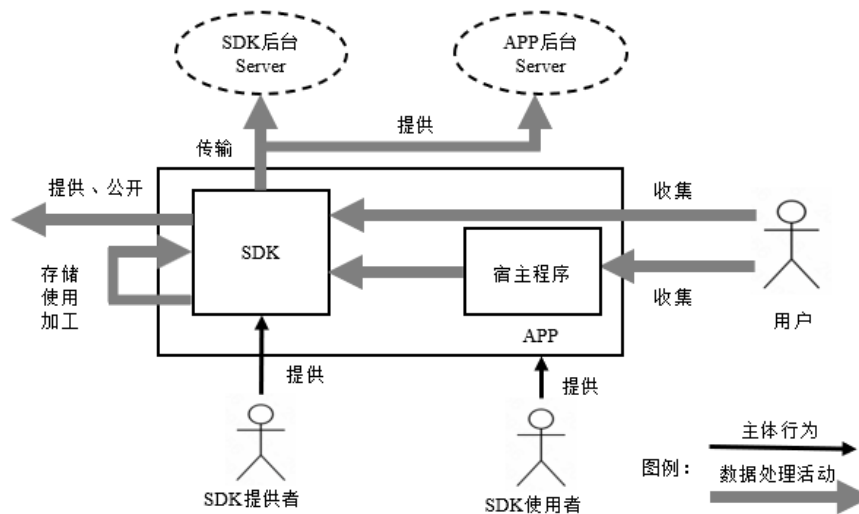


图1 SDK处理个人信息数据流转框架图

5.2 SDK 处理个人信息原则

SDK提供者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括：

- 合法必要：处理个人信息应合法、正当、必要和诚信，不应通过误导、欺诈、胁迫等方式处理个人信息；
- 目的明确：处理个人信息应具有明确、合理的目的，应与处理目的直接相关，应采取对个人权益影响最小的方式；
- 最小必要：收集个人信息时，应当限于实现处理目的的最小范围，不得过度收集个人信息；
- 公开透明：应以明确、清晰、易懂的方式公开个人信息的处理规则；
- 告知同意：应以合理的方式将个人信息的处理目的、方式、范围等规则进行告知，并征得用户同意；若无法独立实现的，SDK使用者应辅助其实现；
- 确保安全：应采取必要的管理措施和技术手段保障所处理的个人信息的安全；
- 主体参与：应向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、投诉等方法；
- 知情自愿：基于用户同意处理个人信息的，该同意应由用户在充分知情的前提下自愿、明确作出。

5.3 SDK 提供者与 SDK 使用者双方义务

SDK处理个人信息或为用户提供服务时，涉及SDK使用者的，应满足以下要求：

- 若SDK使用者与SDK提供者共同处理个人信息，应双方协商确定如何告知用户，征得用户的同意以及提供用户权利保障功能；
- 若SDK提供者，作为受托方，根据SDK使用者的要求处理个人信息，应由SDK使用者告知用户征得用户同意，并提供用户权利保障功能，SDK提供者应协助SDK使用者完成上述义务；
- 若SDK提供者独立处理个人信息的，应自行告知用户，征得用户同意，并提供用户权利保障功能，SDK使用者协助SDK提供者实现相应功能。

6 个人信息处理各环节要求

6.1 个人信息收集要求

6.1.1 个人信息保护政策

SDK提供者的个人信息处理规则应符合以下要求：

- a) SDK提供者应制定个人信息保护政策，包括以下内容：
 - 1) SDK提供者的基本信息，如公司名称或姓名、联系方式等，有法律、行政法规规定应当保密或者不需要告知的情形的可例外；
 - 2) SDK提供者处理个人信息的业务功能，不同业务功能所需的个人信息类型、目的、方式、范围，及其必要性。涉及敏感个人信息的，应明确标识或突出显示，显示方式不限于文字高亮、加粗等方式；
 - 3) SDK提供者安全能力及提供的用户权利保障措施；
 - 4) 对外提供、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任。
- b) 个人信息保护政策的内容应直观、清晰，包括以下要求：
 - 1) 以文档、链接等形式在官网、代码发布平台等位置公开，查询方式应清晰、便捷；
 - 2) 通过合同、集成文档或其他约定形式告知SDK使用者。
注：集成文档可包括个人信息保护政策、开发者手册等形式。
- c) 若SDK涉及处理不满十四周岁未成年人的个人信息，则应制定专门的个人信息处理规则；
- d) 若SDK变更以同意为合法基础的个人信息处理目的、方式、范围的，应当重新征得用户同意，征得用户同意时应满足5.3要求。

6.1.2 SDK 合规指引

SDK提供者应提供合规指引内容，合规指引应符合以下要求：

- a) SDK合规指引内容应包括以下内容：
 - 1) 若涉及个人信息的权限使用，应公开声明功能相关权限使用说明，宜公开声明功能必要性以及缺少该权限所导致的功能限制，非必要功能所涉及权限应提示SDK使用者其非必要性；
 - 2) 若涉及个人信息处理并存在增强功能，如个性化推荐开关、数据收集可选与否、自启动和关联启动开关等，应详细告知SDK使用者功能适配说明等；
 - 3) 为满足SDK个人信息处理合规要求需SDK使用者协助的要求；
 - 4) 宜给SDK使用者提供基础的合规资料参考，如法律法规要求、实践指南等。
- b) SDK合规指引的内容应直观、清晰，可选择下列其中一种或多种方式提供：
 - 1) 以文档、链接等形式在官网、代码发布平台等位置公开，查询方式应清晰、便捷；
 - 2) 通过合同、集成文档或其他约定形式告知SDK使用者。
注：集成文档可包括个人信息保护政策、开发者手册等形式。

6.1.3 权限申请使用要求

SDK的权限申请使用应符合以下要求：

- a) SDK提供者应通过个人信息保护政策等方式简洁、清晰、易懂地声明涉及个人信息的功能所需的权限说明，包括权限的用途；
- b) SDK提供者对权限的申请使用应遵循最小必要原则，不应过度申请使用权限；
- c) SDK提供者在开发过程中应规范权限申请使用，若存在业务功能需申请敏感权限且需SDK使用者协助的，应由SDK使用者主动适配权限申请后实现相应功能。

6.1.4 个人信息收集行为要求

SDK的个人信息收集行为应符合以下要求：

- a) SDK提供者应通过个人信息保护政策等方式简洁、清晰、易懂地声明个人信息处理目的、方式、范围、保存期限等内容；
- b) SDK收集个人信息之前，应征得用户同意或取得处理个人信息的其他合法性基础，征得用户同意应满足5.3要求；
- c) SDK收集个人信息应遵循最小必要原则，应限于实现处理目的的最小范围，应满足以下要求：
 - 1) 收集个人信息的场景、类型、频次均应符合最小必要原则，不应超出个人信息处理规则的范围或实现处理目的的最小范围；
 - 2) 不应频繁收集个人信息，SDK实现业务功能所必需的除外；
 - 3) 应优先在终端本地完成产品或服务的业务功能，若本地无法实现的，再传输回服务器端。
- d) SDK收集敏感个人信息的，应符合以下要求：
 - 1) SDK提供者收集敏感个人信息时，应具有特定目的和充分必要性，并向SDK使用者明示并告知处理敏感个人信息的必要性以及对个人权益的影响；
 - 2) SDK提供者应提供方式和途径向用户告知其处理敏感个人信息的必要性以及对个人权益的影响，告知时应满足5.3要求；
 - 3) SDK提供者应取得用户的单独同意，征得用户同意时应满足5.3要求；
 - 4) SDK提供者收集不满十四周岁未成年人个人信息前，应取得未成年人的父母或者其他监护人的同意，征得用户同意时应满足5.3要求。
- e) SDK提供者自行提供服务时，不得以用户不同意处理个人信息或撤回同意为由，拒绝提供产品或服务。处理个人信息属于提供产品或服务所必需的除外。

6.2 个人信息存储要求

SDK提供者对个人信息存储应符合以下要求：

- a) SDK提供者若在移动智能终端本地存储个人信息，应采取加密或访问控制等安全技术保证个人信息不被破坏或损毁；
- b) SDK提供者应对其服务端存储的个人信息进行分类分级管理，采取不同级别的安全保障措施以确保个人信息在服务器端的安全存储；
- c) SDK使用者和SDK提供者所收集的个人信息存储不应超过实现个人信息主体授权使用的目的所必需的最短时间，不应在用户撤回同意或SDK提供者停止提供产品或服务之后继续存储，但法律法规另有规定或者个人信息主体另行授权同意的除外；
- d) SDK提供者不应将其生成的可用于唯一标识移动智能终端的个人信息存储在移动智能终端本地，并分享给其他SDK使用者用于用户画像或商业营销等目的。

6.3 个人信息使用要求

SDK提供者对个人信息的的使用应符合以下要求：

- a) SDK使用个人信息时，其目的应与告知用户的目的一致。若存在超出的情况，应以站内信、通知公告等方式主动告知SDK使用者和用户，并重新征得用户同意，征得用户同意时应满足5.3要求；
- b) SDK若存在个人信息展示的功能，展示位置包括在官网、SDK使用者前端等，宜对其展示的个人信息采取去标识化处理等措施，如张**替代真实姓名；

- c) SDK若存在利用个人信息通过自动化决策方式向用户进行信息推送或商业营销的功能,为保证满足能够给用户不针对其个人特征的选项或便捷的拒绝方式等要求,应给SDK使用者提供有效的功能说明、个性化推送的开关方式;
- d) 通过自动化决策方式作出对个人权益有重大影响的决定,SDK应提供相关说明,并为用户提供仅通过自动化决策的方式作出决定的拒绝或申诉途径并及时响应。提供用户权利保障时应满足5.3要求。

6.4 个人信息加工要求

SDK提供者对个人信息的加工应符合以下要求:

- a) SDK加工个人信息前,应取得用户的同意,征得用户同意时应满足5.3要求;
- b) 未向用户告知且经用户同意,SDK不得关联分析由不同的SDK使用者收集的个人信息,征得用户同意时应满足5.3要求。

6.5 个人信息传输要求

SDK提供者对个人信息的传输应符合以下要求:

- a) SDK传输个人信息时,应对个人信息进行加密或使用安全的传输协议进行传输;
- b) SDK传输敏感个人信息时,应对个人信息进行加密或使用安全的传输协议的基础上,宜对其采取单独加密等措施。

6.6 个人信息对外提供要求

SDK提供者对外提供个人信息,应符合以下要求:

- a) SDK对外提供个人信息时,应向SDK使用者、用户告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类,并征得用户的单独同意,征得用户同意时应满足5.3要求。接收方变更原先的处理目的、处理方式的,接收方应当重新取得同意,征得用户同意时应满足5.3要求;
- b) SDK提供者委托处理个人信息的,应依据已告知用户的个人信息处理种类、目的、方式进行委托,与受委托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务,准确记录和存储委托处理个人信息情况,必要时对受委托方进行审计;
- c) 因合并、分立、解散、被宣告破产等原因需要转移个人信息的,SDK提供者应向SDK使用者和用户告知接收方的名称或者姓名和联系方式,告知用户时应满足5.3要求。

6.7 个人信息公开要求

SDK提供者公开个人信息,应符合以下要求:

- a) SDK提供者不应公开披露个人信息,若需公开个人信息应取得个人信息主体的单独同意,征得用户同意时应满足5.3要求;
- b) SDK提供者应在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息,用户明确拒绝的除外。处理已公开的个人信息时,对个人权益有重大影响的,应取得用户的同意,征得用户同意时应满足5.3要求。

6.8 个人信息删除要求

SDK提供者删除个人信息,应符合以下要求:

- a) 存储的个人信息在完成其使用业务功能及目的、用户撤回同意、SDK提供者停止提供产品或服务或超出存储期限后，SDK提供者应对个人信息进行删除或匿名化处理，如需SDK使用者协助处理，应满足5.3要求；
- b) 用户提出删除个人信息的请求后，SDK提供者应及时响应用户请求并删除或匿名化个人信息。如需SDK使用者协助处理的，应满足5.3要求。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，SDK提供者应当停止除存储和采取必要的安全保护措施之外的处理。

6.9 个人信息跨境要求

SDK提供者存在将个人信息转移到中华人民共和国境外（包含港澳台地区）的，应符合法律、行政法规和行业主管部门规定的关于个人信息跨境的相关要求，应向SDK使用者和用户告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，基于同意合法基础的数据出境场景需获得用户单独同意，SDK使用者协助SDK提供者实现相应功能，征得用户同意时应满足5.3要求。

7 用户权利保障

用户权利保障相关要求包括：

- a) SDK提供者应为用户提供便捷有效的查阅、复制、更正、补充、删除个人信息的渠道，提供用户权利保障时应满足5.3要求；
- b) SDK提供者基于个人同意处理个人信息的，应为用户提供便捷有效的撤回同意的方式，提供用户权利保障时应满足5.3要求；
- c) 用户申请查阅、复制、更正、补充、删除个人信息或撤回同意的，SDK提供者应及时响应，拒绝用户请求的，应说明理由，提供用户权利保障时应满足5.3要求；
- d) 有下列情形之一的，SDK提供者应主动删除个人信息：
 - 1) 处理目的已实现、无法实现或为实现处理目的不再必要；
 - 2) SDK提供者停止提供产品或服务，或者保存期限已届满；
 - 3) 个人撤回同意；
 - 4) 合作协议约定的情形；
 - 5) SDK提供者违反法律、行政法规或违反约定处理个人信息；
 - 6) 法律、行政法规规定的其他情形。

8 SDK提供者要求

SDK提供者作为个人信息处理者的要求包括：

- a) SDK提供者与第三方共同决定个人信息的处理目的和处理方式的，应当约定好各自的权利和义务；
- b) SDK提供者应建立便捷的个人行使权利的申请受理和处理机制；
- c) SDK提供者应根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，制定内部管理制度和操作规程，制定并组织实施个人信息安全事件应急预案；
- d) SDK提供者应对个人信息实行分类管理；
- e) SDK提供者应采取相应的加密、去标识化等安全技术措施；

- f) SDK 提供者应当定期对处理个人信息遵守法律、行政法规的情况进行合规审计，并形成合规审计记录；
- g) 有下列情形之一的，SDK 提供者应当事前进行个人信息保护影响评估，并对处理情况进行记录：
 - 1) 处理敏感个人信息；
 - 2) 利用个人信息进行自动化决策；
 - 3) 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
 - 4) 向境外提供个人信息；
 - 5) 其他对个人权益有重大影响的个人信息处理活动。
- h) 个人信息影响评估应包含以下内容：
 - 1) 掌握的个人信息数量及个人信息类型；
 - 2) 个人信息的处理目的、处理方式等是否合法、正当、必要；
 - 3) 对个人权益的影响及安全风险；
 - 4) 个人信息处理活动及对应的安全保障措施，包括管理与技术两方面；
 - 5) 是否制定个人信息安全事件的应急响应预案；
 - 6) 所采取的保护措施是否合法、有效并与风险程度相适应。
- i) 个人信息影响评估报告和处理情况记录应至少保存三年；
- j) SDK 提供者应针对下列情形设置相应的管理制度及处理机制：
 - 1) 发生或者可能发生个人信息泄露、篡改、丢失的；
 - 2) 因合并、分立、解散、被宣告破产等原因需要转移个人信息的。

9 评估方法

9.1 个人信息处理各环节的评估

9.1.1 个人信息收集的评估

9.1.1.1 个人信息保护政策的评估

9.1.1.1.1 测试项：详见 6.1.1 a)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 提供者是否制定并公开个人信息保护政策；
 - 2) 查看个人信息保护政策中是否包括以下内容：
 - SDK 提供者的基本信息，如公司名称或姓名、联系方式等，有法律、行政法规规定应当保密或者不需要告知的情形的可例外；
 - SDK 提供者处理个人信息的业务功能，不同业务功能所需的个人信息类型、目的、方式和范围，及其必要性。涉及敏感个人信息的，应在自身个人信息保护政策中或由 SDK 使用者协助在 APP 个人信息保护政策中突出显示，显示方式不限于文字高亮、加粗等方式；
 - SDK 提供者提供的用户权利保障措施；
 - 对外提供、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.1.2 测试项：详见 6.1.1 b)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 提供者是否制定并公开个人信息保护政策；
 - 2) 查看个人信息保护政策是否满足以下要求：
 - 查看个人信息保护政策是否以文档、链接的形式在官网、代码发布平台等位置公开展示；
 - 查看个人信息保护政策是否以合同、集成文档或其他约定的形式告知 SDK 使用者。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.1.3 测试项：详见 6.1.1 c)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 依次查看 SDK 的业务功能，是否涉及处理未满十四周岁未成年人的个人信息；
 - 2) 查看是否制定专门的个人信息处理规则。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为不适用，否则判定步骤 2)；若测试步骤 2) 结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.1.4 测试项：详见 6.1.1 d)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档审查、功能检查等方式，判断 SDK 是否变更以同意为合法基础的个人信息处理目的、方式、范围；
 - 2) 查看 SDK 是否重新取得用户同意。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常，否则判定步骤 2)；若测试步骤 2) 结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.2 SDK 合规指引的评估

9.1.1.2.1 测试项：详见 6.1.2 a)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 提供者是否提供合规指引；
 - 2) 依次确认 SDK 业务功能，判断 SDK 是否申请使用涉及个人信息的权限；
 - 3) 依次确认 SDK 业务功能，判断 SDK 是否存在增强功能；
 - 4) 查看 SDK 合规指引中是否包括权限使用说明；
 - 5) 查看 SDK 合规指引是否包括增强功能（如个性化推荐开关、数据收集可选、自启动与关联启动开关等）适配及使用说明；
 - 6) 查看是否包含为满足个人信息处理安全要求需 SDK 使用者协助的要求。
- c) 结果判定：若以上测试步骤结果均为是，则测试项判定为未见异常；若步骤一结果为是，步骤二结果为否，则跳过步骤四；若步骤三为否，则跳过步骤五，步骤六结果为是，则测试项判定为未见异常；其他情况则判定为不符合要求。

9.1.1.2.2 测试项：详见 6.1.2 b)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 提供者是否制定并公开 SDK 合规指引；
 - 2) 查看 SDK 合规指引是否满足以下其中一种形式：
 - 查看 SDK 合规指引是否以文档、链接的形式在官网、代码发布平台等位置公开展示；
 - 查看 SDK 合规指引是否以合同、集成文档或其他约定的形式告知 SDK 使用者。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.3 权限申请使用的评估

9.1.1.3.1 测试项：详见 6.1.3 a)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 提供者是否提供个人信息保护政策；
 - 2) 查看个人信息保护政策中是否简洁、清晰、易懂地声明涉及个人信息的功能所需的权限，包括权限用途及其必要性。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.3.2 测试项：详见 6.1.3 b)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：依次查看 SDK 业务功能申请的权限列表，判断是否在权限申请使用上遵循最小必要原则；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.3.3 测试项：详见 6.1.3 c)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档审查、人员访谈等形式，查验 SDK 提供者在开发过程中是否规范申请使用权限；
 - 2) 对应业务功能查验代码、设计文档等，查看 SDK 申请的权限列表是否涉及敏感权限申请，权限申请使用是否由 SDK 使用者主动申请适配以实现相应功能。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.4 个人信息收集行为的评估

9.1.1.4.1 测试项：详见 6.1.4 a)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 提供者是否提供个人信息保护政策；
 - 2) 查看个人信息保护政策中是否简洁、清晰、易懂地声明涉及个人信息的处理目的、方式、范围以及保存期限等内容。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.4.2 测试项：详见 6.1.4 b)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 是否存在个人信息收集行为；
 - 2) 通过检测工具、文档审查等方式，查看 SDK 收集个人信息的行为是否经用户同意或具备其他合法性依据。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常。若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.4.3 测试项：详见 6.1.4 c)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 依次查看 SDK 功能，通过检测工具查看不同业务功能下所收集个人信息的种类、频次，是否超出约定范围或实现处理目的的最小范围；
 - 2) 判断 SDK 是否频繁收集个人信息；
 - 3) 查看 SDK 的业务功能，是否存在可在本地完成的功能，仍将个人信息传输回服务器。
- c) 结果判定：若以上测试步骤结果为否，则测试项判定为未见异常，否则判定为不符合要求。

9.1.1.4.4 测试项：详见 6.1.4 d)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 依次查验 SDK 各项业务功能，是否涉及敏感个人信息收集；
 - 2) 查看各项业务功能收集敏感个人信息是否具有特定目的和必要性，是否向 SDK 使用者明示告知处理敏感个人信息的必要性和对个人权益的影响；
 - 3) 查看 SDK 提供者如 APP 是否提供方式和途径，向用户告知 SDK 处理敏感个人信息的必要性；
 - 4) 查看 SDK 提供者是否获取用户的单独同意，获得用户用户同意的方式是否参照 5.3 要求；
 - 5) 查看 SDK 提供者是否涉及不满十四周岁的未成年人个人信息的处理；
 - 6) SDK 收集不满十四周岁未成年人个人信息前，查看是否取得未成年人父母或其他监护人同意，获得同意方式是否参照 5.3 要求。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若步骤 1) 到步骤 4) 结果均为是，步骤五为否，则测试项判定为未见异常；若以上测试步骤结果均为是，则测试项判定为未见异常；其他情况则判定为不符合要求。

9.1.1.4.5 测试项：详见 6.1.4 e)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 是否存在个人信息收集行为；
 - 2) 依次查验 SDK 业务功能，判断 SDK 是否因用户不同意处理个人信息或撤回同意为由，拒绝提供产品或服务，无法正常使用产品功能或服务。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常。若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.2 个人信息存储的评估

9.1.2.1 测试项：详见 6.2 a)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 业务功能，是否涉及在移动智能终端本地存储个人信息的功能；
 - 2) 查看移动智能终端本地存储的文本文件、缓存、数据库等，是否包含个人信息；
 - 3) 若包含个人信息，则查看是否对个人信息进行加密，或者对文件设置访问权限等安全技术措施。
- c) 结果判定：若测试步骤 1) 结果为否或测试步骤 2) 结果为否，则测试项判定为未见异常。若以上测试步骤结果均为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.2.2 测试项：详见 6.2 b)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档核验、人员访问、服务端核验等多种方式判断 SDK 服务端是否对个人信息进行分类分级管理；
 - 2) 不同等级的个人信息是否采取不同的安全保障措施，如采用不同等级的加密方式、不同等级的权限设计等。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.2.3 测试项：详见 6.2 c)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过文档核验、人员访问、服务端核查、技术验证等多种方式查看 SDK 服务端个人信息存储期限是否是个人信息主体授权目的所必需的最短时间
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.2.4 测试项：详见 6.2 d)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档核验、人员访问、技术验证等多种方式查看 SDK 是否存在生成可用于唯一标识移动智能终端的个人信息；
 - 2) 通过技术验证的方式查看 SDK 是否未将该信息存储在移动智能终端本地且未分享给其他 SDK 使用者用于用户画像或商业营销等目的。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.3 个人信息使用的评估

9.1.3.1 测试项：详见 6.3 a)

- a) 前置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档审查、功能核验、服务端核查等方式，判断 SDK 使用个人信息时，其目的是否与告知用户的目的一致；
 - 2) 若存在超出的情况，需确认是否以站内信、通知公告等方式主动告知 SDK 使用，是否保留相关记录。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.3.2 测试项：详见 6.3 b)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 是否存在个人信息展示的功能；
 - 2) 查看个人信息是否采取去标识化、掩码等措施处理。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若以上步骤测试结果是为，则测试项判定为未见异常，否则判定为不符合要求。

9.1.3.3 测试项：详见 6.3 c)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 是否存在利用个人信息通过自动化决策方式向用户进行信息推送或商业营销的功能；
 - 2) 查看 SDK 提供者是否给 SDK 使用者提供有效的功能说明、个性化推送开关方式等。
- c) 结果判定：若以上测试步骤结果是为，则测试项判定为未见异常，否则判定为不符合要求。

9.1.3.4 测试项：详见 6.3 d)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 是否存在通过自动化决策方式作出对个人权益有重大影响的决定；
 - 2) SDK 提供者是否提供相关说明，并为用户提供仅通过自动化决策的方式作出决定的拒绝或申诉途径并及时响应，提供用户权利保障时是否满足 5.3 要求。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若以上步骤测试结果是为，则测试项判定为未见异常，否则判定为不符合要求。

9.1.4 个人信息加工的评估

9.1.4.1 测试项：详见 6.4 a)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档审核、问卷调查等方式，查看 SDK 是否会加工个人信息；
 - 2) SDK 对个人信息的加工情况，是否征得用户同意，是否满足 5.3 要求。
- c) 结果判定：若以上步骤测试结果是为，则测试项判定为未见异常，否则判定为不符合要求。

9.1.4.2 测试项：详见 6.4 b)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档审核、问卷调查、技术验证等方式，查看 SDK 是否关联分析由不同的 SDK 使用者收集的个人信息；
 - 2) SDK 关联分析由不同的 SDK 使用者收集个人信息的情况，是否告知用户并征得用户同意，征得用户同意时是否满足 5.3 要求。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若以上步骤测试结果是为，则测试项判定为未见异常，否则判定为不符合要求。

9.1.5 个人信息传输的评估

9.1.5.1 测试项：详见 6.5 a)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过网络抓包等其他技术方式，查看 SDK 传输个人信息时，是否使用 HTTPS 协议传输协议或对个人信息进行加密；
- c) 结果判定：若步骤测试结果是为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.5.2 测试项：详见 6.5 b)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过网络抓包等其他技术方式，查看 SDK 传输敏感个人信息时，是否在安全传输协议的基础上，对敏感个人信息单独加密；
- c) 结果判定：若步骤测试结果是为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.6 个人信息对外提供的评估

9.1.6.1 测试项：详见 6.6 a)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 是否对外提供个人信息；
 - 2) 查看 SDK 是否向用户告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并征得用户及 SDK 使用者的单独同意；
 - 3) 查看是否存在接收方变更原先的处理目的、方式的情况；
 - 4) 查看 SDK 是否重新获得用户同意，征得用户同意是否满足 5.3 要求。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若步骤 1) 和步骤 2) 结果为是，步骤 3) 结果为否，则测试项判定为未见异常；若以上测试步骤结果为是，则测试项判定为未见异常，其他情况判定为不符合要求。

9.1.6.2 测试项：详见 6.6 b)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 查看 SDK 是否委托处理个人信息；
 - 2) 查看 SDK 是否依据已告知用户的个人信息处理种类、目的、方式进行委托；
 - 3) 查看是否与受委托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务，准确记录和存储委托处理个人信息情况；
 - 4) 查看是否存在必要时，对受委托方的审计机制和审计记录。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.1.6.3 测试项：详见 6.6 c)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：

- 1) 通过文档核验等方式,查看 SDK 是否具备因合并等情况出现而转移个人信息的制度和流程文档;
- 2) 查看是否包括 SDK 应向用户告知接收方的名称或姓名,联系方式等内容。
- c) 结果判定:若以上测试步骤结果为是,则测试项判定为未见异常,否则判定为不符合要求。

9.1.7 个人信息公开的评估

9.1.7.1 测试项:详见 6.7 a)

- a) 预置条件:被测 SDK 处于正常状态,被测 SDK 涉及个人信息处理;
- b) 测试步骤:
 - 1) 查看 SDK 提供者是否公开披露个人信息;
 - 2) 查看 SDK 提供者是否存在单独获取个人信息主体同意的形式或记录等。
- c) 结果判定:若测试步骤 1) 结果为否,则测试项判定为未见异常;若以上测试步骤结果为是,则测试项判定为未见异常,否则判定为不符合要求。

9.1.7.2 测试项:详见 6.7 b)

- a) 预置条件:被测 SDK 处于正常状态,被测 SDK 涉及个人信息处理;
- b) 测试步骤:
 - 1) 查看 SDK 提供者是否存在公开披露个人信息的情况;
 - 2) 查看是否存在处理已公开个人信息的合理范围的评估机制及要求,确保 SDK 提供者在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;
 - 3) 查看是否存在处理已公开个人信息情况,对个人权益是否有重大影响的评估机制或记录等,查看记录中是否取得用户的同意。
- c) 结果判定:若测试步骤 1) 结果为否,则测试项判定为未见异常;若以上测试步骤结果为是,则测试项判定为未见异常,否则判定为不符合要求。

9.1.8 个人信息删除的评估

9.1.8.1 测试项:详见 6.8 a)

- a) 预置条件:被测 SDK 处于正常状态,被测 SDK 涉及个人信息处理;
- b) 测试步骤:通过文档审核、技术检测、服务端查验等方式,查看存储的个人信息在完成其使用业务功能及目的、用户撤回同意、SDK 提供者停止提供产品或服务、或超出存储期限后,是否被删除或匿名化处理;
- c) 结果判定:若测试步骤结果为是,则测试项判定为未见异常,否则判定为不符合要求。

9.1.8.2 测试项:详见 6.8 b)

- a) 预置条件:被测 SDK 处于正常状态,被测 SDK 涉及个人信息处理;
- b) 测试步骤:
 - 1) 通过文档审核、功能查验等方式,查看用户提出删除请求后,SDK 提供者是否会在十五个工作日内及时响应用户请求;
 - 2) 若用户删除请求符合正常删除范围的,是否按照用户要求尽快删除或匿名化;
 - 3) 若删除用户个人信息在技术上无法实现的,是否采用去标识、停止存储访问和使用等多种保护措施确保个人信息不被使用。
- c) 结果判定:若以上测试步骤结果为是,则测试项判定为未见异常,否则判定为不符合要求。

9.1.9 个人信息跨境的评估

9.1.9.1 测试项：详见 6.9

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 通过文档审查、技术验证等方式，检测 SDK 发起的网络请求，查看域名解析结果，判定 SDK 是否存在将个人信息转移到中华人民共和国境外的情况；
 - 2) 查看是否向 SDK 使用者、用户告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项；
 - 3) 查看基于同意合法基础的数据出境场景是否获得用户单独同意，征得用户同意时是否满足 5.3 要求。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.2 用户权利保障的评估

9.2.1 测试项：详见 7 a)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验、功能验证等方式，检查 SDK 是否按照 5.3 要求结合自身角色（如独立的个人信息处理者或受托方）为用户提供便捷有效的查阅、复制、更正、补充、删除个人信息的渠道；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.2.2 测试项：详见 7 b)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验、功能验证等方式，确定 SDK 提供者基于个人同意处理个人信息时，检查其是否按照 5.3 要求结合自身角色为用户提供便捷有效的撤回同意的方式，例如，打开撤回同意开关、关闭或禁用相应业务功能等；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.2.3 测试项：详见 7 c)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 模拟用户操作，向 SDK 申请查阅、复制、更正、补充、删除个人信息或撤回同意，检查 SDK 是否及时响应；
 - 2) 检查请求被拒绝时，SDK 是否说明了具体理由。
- c) 结果判定：若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.2.4 测试项：详见 7 d)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者在以下情形下，是否存在主动删除个人信息的情况：
 - 1) 处理目的已实现、无法实现或为实现处理目的不再必要；

- 2) SDK 停止提供产品或服务，或者保存期限以届满；
 - 3) 个人撤回同意；
 - 4) 合作协议约定的情形；
 - 5) SDK 违反法律、行政法规或违反约定处理个人信息。
 - 6) 法律、行政法规规定的其他情形。
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3 SDK 提供者的评估

9.3.1 测试项：详见 8 a)

- a) 预置条件：被测 SDK 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：
 - 1) 检查 SDK 是否存在与第三方共同决定个人信息的处理目的和处理方式的情况；
 - 2) 检查 SDK 与第三方是否约定好各自的权利和义务。
- c) 结果判定：若测试步骤 1) 结果为否，则测试项判定为未见异常；若以上测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。。

9.3.2 测试项：详见 8 b)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验、功能验证等方式，检查 SDK 是否建立了便捷的个人行使权利的申请受理和处理机制；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.3 测试项：详见 8 c)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者是否根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，制定了内部管理制度和操作规程，制定并组织实施了个人信息安全事件应急预案；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.4 测试项：详见 8 d)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者是否对个人信息实行了分类管理；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.5 测试项：详见 8 e)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验、功能验证等方式，检查 SDK 提供者是否采取了相应的加密、去标识化等安全技术措施；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.6 测试项：详见 8 f)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者是否定期对处理个人信息遵守法律、行政法规的情况进行合规审计，并形成合规审计记录；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.7 测试项：详见 8 g)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者在以下情形下，是否在事前进行了个人信息保护影响评估，并对处理情况进行记录：
 - 1) 处理敏感个人信息；
 - 2) 利用个人信息进行自动化决策；
 - 3) 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
 - 4) 向境外提供个人信息；
 - 5) 其他对个人权益有重大影响的个人信息处理活动。
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.8 测试项：详见 8 h)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者的个人信息影响评估是否包含以下内容：
 - 1) 掌握的个人信息数量及个人信息类型；
 - 2) 个人信息的处理目的、处理方式等合法、正当、必要；
 - 3) 对个人权益的影响及安全风险；
 - 4) 个人信息处理活动及对应的安全保障措施，包括管理与技术两方面；
 - 5) 制定个人信息安全事件的应急响应预案；
 - 6) 所采取的保护措施合法、有效并与风险程度相适应；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.9 测试项：详见 8 i)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者的个人信息影响评估报告和处理情况记录是否至少保存三年；
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

9.3.10 测试项：详见 8 j)

- a) 预置条件：被测 SDK 及宿主 APP 处于正常状态，被测 SDK 涉及个人信息处理；
- b) 测试步骤：通过问询、文档审核、系统查验等方式，检查 SDK 提供者是否针对下列情形设置相应的管理制度及处理机制：
 - 1) 发生或者可能发生个人信息泄露、篡改、丢失的；
 - 2) 因合并、分立、解散、被宣告破产等原因需要转移个人信息的。
- c) 结果判定：若测试步骤结果为是，则测试项判定为未见异常，否则判定为不符合要求。

电信终端产业协会团体标准
软件开发包（SDK）个人信息处理规范

T/TAF 123—2022

*

版权所有 侵权必究

电信终端产业协会印发

地址：北京市西城区新街口外大街 28 号

电话：010-82052809

电子版发行网址：www.taf.org.cn